

Title: Unauthenticated Information Disclosure

Risk: High

Effectuated Components: Search

Scope of Test: Discovered Internally

Note: Vulnerability may affect more than accessing retail-operator-admin-tool/retail-operator-admin-tool.

CVSS Risk Score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Recommendation:

It is highly recommended to ensure that authenticated and authorized users only can access the application features.

Impact:

Unauthenticated users can access critical information such as Retail-operator-admin-tool that lists a Docker image with a list of vulnerabilities CVEs and the vulnerable packages so malicious user can build a list of exploits that affect the system.

The vulnerability affects confidentiality since it allows attackers to know a list of docker images, technologies used such as OS and libraries, most of them effects encryption and system availability.

Exploit Scenario:

1- Malicious user will access the Harbor URL

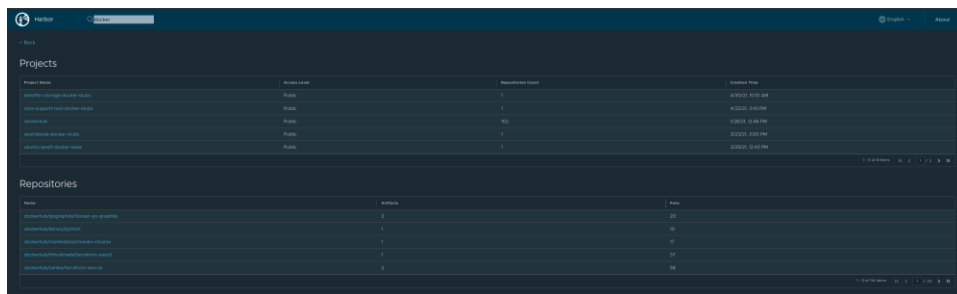
https://harbor-main.example.com/account/sign-in?redirect_url=%2Fharbor%2Fprojects



Figure01: screenshot shows the home of harbor page.

2- Malicious users will search for admin in search bar

- 5- Other pages Unauthenticated user may have access to it such as
- Dockerhub/*

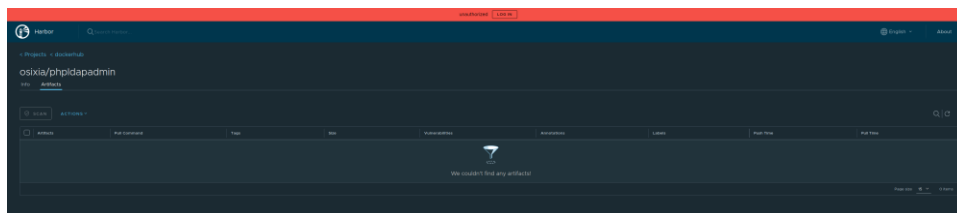


The screenshot shows the Docker Hub search results for the term 'docker'. It displays two sections: 'Projects' and 'Repositories'. The 'Projects' section lists several projects with columns for Project Name, Docker Hub ID, Repository Count, and Created Time. The 'Repositories' section lists repositories with columns for Name, Stars, and Pulls.

| Project Name | Docker Hub ID | Repository Count | Created Time |
|--------------|---------------|------------------|---------------------|
| docker-ce | docker | 1 | 2015/01/10 10:00:00 |
| docker-ce | docker | 1 | 2015/01/10 10:00:00 |
| docker-ce | docker | 1 | 2015/01/10 10:00:00 |
| docker-ce | docker | 1 | 2015/01/10 10:00:00 |
| docker-ce | docker | 1 | 2015/01/10 10:00:00 |

| Name | Stars | Pulls |
|---------------------|-------|-------|
| osixia/phpldapadmin | 2 | 20 |
| osixia/phpldapadmin | 1 | 10 |
| osixia/phpldapadmin | 1 | 10 |
| osixia/phpldapadmin | 1 | 10 |
| osixia/phpldapadmin | 1 | 10 |

Figure06: Screenshot show a search result for Docker



The screenshot shows the Docker Hub repository page for 'osixia/phpldapadmin'. It displays the repository name, a description, and a table of tags. The table has columns for Tag, Architecture, and Size. The 'latest' tag is highlighted.

| Tag | Architecture | Size |
|--------|--------------|--------|
| latest | amd64 | 10.5MB |
| 1.0.0 | amd64 | 10.5MB |
| 1.0.1 | amd64 | 10.5MB |
| 1.0.2 | amd64 | 10.5MB |
| 1.0.3 | amd64 | 10.5MB |

Figure07: Screenshot shows the page of osixia/phpldapadmin under dockerhub